

CALIFORNIA DEPARTMENT OF CHILD SUPPORT SERVICES

P.O. Box 419064, Rancho Cordova, CA 95741-9064



February 3, 2016

CSS LETTER: 16-02

ALL IV-D DIRECTORS
ALL COUNTY ADMINISTRATIVE OFFICERS
ALL BOARDS OF SUPERVISORS

SUBJECT: NEW INFORMATION SECURITY MANUAL, ACCESS CONTROL
STANDARD – SINGLE SIGN-ON AND TWO-FACTOR
AUTHENTICATION

<u>Reason for this Transmittal</u>
<input type="checkbox"/> State Law, Regulation and/or Change
<input type="checkbox"/> Federal Law, Regulation and/or Change
<input type="checkbox"/> Court Order or Settlement Change
<input type="checkbox"/> Clarification requested by One or More Counties
<input checked="" type="checkbox"/> Initiated by DCSS

The Department of Child Support Services (DCSS) has added two new components to the Information Security Manual (ISM) 6001 Access Control Standard. Access controls are security measures for ensuring that only users with the proper business need and authority can access the systems that process or store child support information and perform authorized functions. The new components are:

- **Single Sign-On Systems.** This new standard improves security mechanisms that allow a user to authenticate one authority and access multiple applications or systems utilizing a user ID and password.
- **Two-Factor Authentication.** This new standard creates a method of using two factors of information for authentication, utilizing a token or biometric feature as the second factor.

The ISM is available on California Child Support Central or can be requested by contacting the ISO mailbox: info.security@dcss.ca.gov.

If you have any questions or concerns regarding this matter, please contact John Cleveland, DCSS Information Security Officer at (916) 464-5045.

Sincerely,

O/S

JOHN CLEVELAND
Chief Information Security Officer

Attachment: ISM 6001 Access Control Standard

ISM 6001 - Access Control Standard

Access controls are measures for ensuring that only users with the proper need and authority can access the system and perform authorized functions on the systems containing child support information. Applicable organizations' management and staff must understand their responsibilities relative to access control. This access control standard contains the following directives:

- Access Control Rules
- Requirements for Access Control
- User Access Management
- Application Access Control
- Monitoring-System Access and Use

Access Control Rules

Access to child support information and information assets will be managed using two complementary security principles: The "need to know" and the "least privilege." Access control should start by denying access to everything, and then explicitly granting access according to the "need to know" principle. Child support employees should be granted access to child support information or child support information assets necessary to carry out Child Support Program responsibilities. Access to child support information and child support information assets should be based on the principle of "least privilege," that is, grant no user greater access privileges to the information or assets than Child Support Program responsibilities require.

The "least privilege" principle should also be applied to users' modes of access, such as whether the individual is granted "read or write" privileges.

Requirements for Access Control

These access control requirements apply to any system that processes or stores child support information and child support information assets.

System Requirements

Any system that processes or stores child support information will:

- Meet the ISM 6002 - Password Standard.
- Strictly control access enabling only privileged users or supervisors to override system controls or the capability of bypassing data validation on editing problems.
- Monitor special privilege access, such as administration accounts.
- Restrict authority to change master files to persons independent of the data

processing function.

- Have access control mechanisms to prevent unauthorized access or changes to data, especially the server file systems that are connected to the Internet, even behind a firewall.
- Be capable of routinely monitoring the access to automated systems containing child support information.
- Log all modifications to the system files.
- Limit access to system utility programs to necessary individuals with specific designation.
- Maintain audit logs on a device separate from the system being monitored.
- Delete or disable all default accounts.
- Restrict access to server file-system controls to ensure that all changes such as direct write, write access to system areas, and software or service changes will be applied only through the appropriate change control process.
- Restrict access to server-file-system controls that allow access to other users' files.
- Ensure that servers containing user credentials will be physically protected, hardened, and monitored to prevent inappropriate use.

Log-on Banners and Warning Notices

All computer systems that contain or access child support information will display warning banners of conditions of use consistent with state and federal laws.

Warning banners must remain on the screen until the user takes explicit actions to log on to the information system.

The banner message will be placed at the user authentication point for every computer system that contains or accesses child support information. The banner message may be placed on an initial logon screen in situations where the logon provides access to multiple computer systems.

At a minimum, banner messages must provide appropriate privacy and security information and shall contain information informing potential users that:

- User is accessing a government information system under conditions of use consistent with state and federal information security and privacy protection laws.
- System usage may be monitored, recorded, and subject to audit.
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
- Use of the system indicates consent to monitoring and recording.

User Access Management

This section describes the user access lifecycle from granting user access to termination of access.

User Identification and Authentication

Access control is the process of limiting and controlling access to system resources, and user identification (ID) and authentication is the most fundamental aspect to control access.

Applicable organizations' management will ensure that systems that contain or store child support information will:

- Uniquely identify each individual user.
- Authenticate user identities at logon. Authentication mechanisms will be appropriate to the sensitivity of the information.
- Provide accountability for each user's activity using child support information.

Single Sign-On Systems

Single Sign-On (SSO) systems are mechanisms that allow a user to authenticate to one authentication authority and gain access to multiple applications or systems that have different authentication mechanisms. User credentials for their multiple applications are usually stored and securely managed by the SSO system. Although SSO systems could provide a vector for unauthorized access if compromised, properly implemented and maintained SSO systems can provide additional security in the form of two-factor authentication and fewer forgotten passwords.

All SSO systems must meet State Leadership Accountability Act (SLAA) (formerly known as Federal Information Security Management Act (FISMA)) and Federal Risk and Authorization Management Program (FedRAMP) standards.

Additionally, the following are required controls for implementing SSO systems:

- The controlling authentication mechanism for any SSO system must be fronted with some form of two-factor authentication that is SLAA and FedRAMP compliant. (as defined in 44 U.S.C. § 3541, et seq).
- If credentials are stored, they must be encrypted with FIPS 140-2 validated cryptographic modules.
- Stored credentials cannot be accessible by administrators of the system.

Two Factor Authentication

Two Factor Authentication, or 2FA, is a method of using two separate pieces of information for authentication. These are generally said to be something you have, and something you know. In single-factor authentication, a user ID and password are things you know. With 2FA, a token or biometric feature is used as the second factor as something you have. Please note: employing the use of two separate user ID's and passwords does not meet this standard.

The Internal Revenue Service and Office of Child Support Enforcement both require Two Factor Authentication for all remote access to Child Support and Federal Tax Information. Remote access is defined as any access outside of the Local Area Network (LAN) of the Child Support Agency.

User Registration

User registration is a process that documents access levels authorized for each child support employee. It ensures user identity and the need to access child support information and child support information assets. Applicable organizations' management will establish and maintain user registration procedures that apply to all stages of user access life cycle, from registration of new users to de-registration of users no longer authorized to have access. The user registration procedures will:

- Track or document which individuals are authorized to issue user IDs to child support employees and restrict authority to issue user IDs to those identified individuals.
- Track or document the access control level privileges that may be granted and restrict individuals' access to authorized levels.
- Track or document the access levels granted to each registered child support employee.
- Conduct regular reviews of the registered child support employees' access level privileges.
- Provide procedures to disable user accounts upon termination of employment or contractual obligation, and procedures to modify access privileges upon change in job responsibilities.
- Secure password delivery and password reset mechanisms to assure passwords are known only to the user.

Account and Access Management

The following account and access management processes applies to all applicable organizations:

- Child support employees should be assigned only the access privileges needed for their job.
- For any system that processes or stores child support information, password security will extend to the functional screen level and limit the user's capability to view and/or update those screens.
- System administration accounts should be assigned and used only for performing administrative activities. For example, do not log-in with administrative account when using the system as a regular user, not performing administrative duties.
- Each user will have a unique user ID. Accounts should NOT be shared at any time.
- Child support employees should log off or activate password-protected mechanisms (e.g., password-protected screensavers) before leaving the immediate vicinity of child support systems whenever possible.

Inactivity Timeout and Restricted Connection Times

Systems that process or store child support information shall implement the following:

- Automatic lockouts for system devices, including workstations or other mobile computing devices, after no more than 10 minutes of inactivity. Refer to ISM 9006 - Mobile Computing Device Standard.
- Automatic network session termination for network connections associated with a communications session at the end of a session after no more than 10 minutes of inactivity.

Application Access Control

For any system that processes or stores child support information, controls should be used to restrict access within application systems. Logical access to software and information should be limited to authorized users only. Application system controls should:

- Control user access to information and application system functions, according to a defined access-control policy.
- Prevent unauthorized access to any utility or operating-system software that can override system or application controls.

- Prevent compromise to the security of other systems with which information resources are shared.
- Allow access only to the owner of information and other authorized users or groups.
- Carefully manage all interfaces.
- Provide security levels for access to records and files.

Monitoring-System Access and Use

See ISM 9004 - Secure System Standard, for system monitoring requirements.